Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act Of 1996	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	
	)	
IP-Enabled Services	)	WC Docket No. 04-36
	)	

JOINT COMMENTS OF NUVOX COMMUNICATIONS AND XO COMMUNICATIONS, LLC

NuVox Communications and XO Communications, LLC (collectively, "Joint Commenters"), through their undersigned counsel and in response to the Federal Communications Commission's ("Commission") Further Notice of Proposed Rulemaking ("FNPRM"),[1] respectfully submit these comments in the above-captioned proceeding. Joint Commenters have adopted stringent safeguards to protect the use and disclosure of customer proprietary network information ("CPNI"), and, to the best of their knowledge, have prevented unauthorized individuals from obtaining access to CPNI. The Commission's recently adopted requirements provide more than adequate protection against pretexting and other

[1] *Implementation of the Telecommunications Act of 1996, Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. Apr. 2, 2007). For simplicity, we will refer to the order portion of FCC 07-22 as the "Report and Order" and the further notice portion of FCC 07-22 as the "FNPRM."

unauthorized access to CPNI. Accordingly, there is no need to adopt any of the additional CPNI-related regulations discussed in the FNPRM. The costs and burdens that such regulations would impose on carriers and consumers far outweigh any perceived benefit they could have in addressing a problem that the Commission already has addressed and that Congress has criminalized.[2] Moreover, the high costs of implementing these proposals necessarily would be passed onto consumers. At a minimum, it would be premature to adopt changes without first giving the new CPNI regulations and law a chance to go into effect and to be enforced by the Commission and the appropriate law enforcement personnel.

I. THE COMMISSION SHOULD NOT ADOPT MORE BURDENSOME PASSWORD REQUIREMENTS

Joint Commenters oppose the extension of in-bound calling password requirements (either mandatory or optional) to non-call detail information.[3] The Commission recently required the use of passwords for the release of call detail information on in-bound calls.[4] No basis exists for expanding this requirement to the release of any other information on in-bound calls. The record contains no evidence that pretexting or similar problems exist with respect to unauthorized access to non-call detail CPNI. Further, as explained below, there are compelling reasons for affirmatively rejecting the proposed extension of password requirements

---

2 *See* Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476 (Jan. 12, 2007).

3 FNPRM ¶ 68 (seeking comment on whether the Commission should extend password rules for all non-call detail CPNI or for certain (unspecified) account changes).

4 *See* Report and Order ¶ 13.

beyond those already adopted by the Commission. The costs and burdens of expanding the password requirement to include non-call detail information would outweigh any perceived benefit.

Requiring passwords for non-call detail CPNI on in-bound calls would frustrate the legitimate transfer of information between carriers and their customers, create dissatisfaction for consumers, and impose undue costs and burdens on carriers – all without any measurable benefit in terms of thwarting unauthorized access to non-call detail CPNI. The record in this proceeding demonstrates that customers do not want their account information password protected on in-bound calls.[5] Expanded password requirements only would serve to impose additional hurdles between customers and the information they legitimately seek, and would deter—if not prevent—carriers from making information available during an in-bound call. Such requirements also would cause delay and would inconvenience consumers and businesses seeking legitimate access to their own CPNI.

The costs and burdens involved with implementing passwords, particularly for business customers, in a live-call environment are substantial.[6] Requiring passwords for business customers to access non-call detail information would be particularly unworkable. This is largely because business customers

---

5 *See id.* at note 47 (stating, "[w]e understand that many consumers may not like passwords…") (citations omitted).

6 There are also costs involved with redirecting customers. Most prominently, these costs may register initially in terms of a decline in customer satisfaction or an inability to obtain higher levels of customer satisfaction. Increased customer dissatisfaction often leads to churn. Churn is very costly to carriers, especially to CLECs serving business customers.

typically have multiple authorized administrators on a single account, and, consequently, have difficulty keeping track of their current password. Business customers also must request that their password(s) be reset each time an employee with access leaves and a new person who is to have access begins employment.[7] Moreover, the hardware and software development, procurement, installation and maintenance costs, increased call times, labor costs, and resources for training development and implementation are all substantial. Optional passwords potentially would impose greater costs and burdens on carriers. Indeed, optional passwords would require carriers to maintain two systems and two sets of procedures for authentication.

Since the Commission last sought comment, no facts have emerged to justify passwords for non-call detail information nor have the costs and burdens associated with expanded passwords changed.[8] Customers dislike barriers to

---

7 *See also* Ex Parte letter to Marlene Dortch, Secretary, Federal Communications Commission, from John J. Heitmann and Jennifer M. Kashatus, Kelley Drye & Warren LLP, at 3 (Nov. 7, 2006) (on behalf of XO Communications) (stating that, in the business context, the effectiveness of passwords are highly dependent on the security culture of the particular business customers, and that multiple points of access, lax customer protocols, and potential password compromise significantly increase the burdens associated with the use and implementation of passwords for business customers).

8 *See, e.g.,* Joint Reply Comments of Eschelon Telecom, Inc., SNiP LiNK Inc., and XO Communications, Inc. at 3-5 (stating that passwords are burdensome and costly to implement and that the great costs and burdens associated with implementing consumer-set passwords out outweigh any appreciable consumer security benefit); Comments of Time Warner Telecom at 12 (stating that consumer-set passwords are troublesome for business customers, because if one person in the company forgets the password, then the entire company password system must be reset).

accessing their own information.[9] Indeed, *passwords have not been proven more effective than existing measures that carriers have adopted to prevent unauthorized access to CPNI*. The imposition of an expanded password requirement risks undermining the effective authentication practices many carriers already use and further risks the abandonment of those proven methods of secure access to data. In light of the costs and burdens associated with the expanded password proposal to address a problem that does not exist, the Commission should not alter the existing password regulations to encompass non-call detail CPNI.

II. REQUIRING CARRIERS TO IMPLEMENT AUDIT TRAILS WOULD NOT BENEFIT LAW ENFORCEMENT ACTIVITY

The record reflects that "the broad use of audit trails likely would be of limited value in ending pretexting because such a log would record enormous amounts of data, the vast majority of it being legitimate customer inquiry."[10] It remains the case today that audit trails are of limited use. Carriers and the Commission all have previously acknowledged the extreme cost and burden to implement audit trails.[11] For these reasons, the Commission has refused to adopt an audit trail requirement and should do so again here especially where the burden and cost significantly outweigh any perceived benefit.[12]

---

9 *See* Report and Order at note 47 (stating, "[w]e understand that many consumers may not like passwords…") (citations omitted).

10 FNPRM ¶ 69.

11 *See id.* (noting that the record indicates that audit trails would be costly to implement with "little to no corresponding benefit to the consumer").

12 *Id.; see also Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-*

Notably, the interests of law enforcement support this result. Law enforcement personnel have stated that the use of an audit trail could hinder federal investigations. In discussing the foreign storage of data, the FBI indicated that a carrier's use of an audit trail could "compromise an important investigation."[13] This is likely the case because an audit trail also would reveal *all* requests for CPNI, *including* those made by law enforcement. The record to date contains no evidence that the adoption of an audit trail requirement is necessary to assist law enforcement personnel in their criminal investigations against pretexters or that law enforcement is having difficulty obtaining access to carrier information that may be relevant to instances of pretexting. Subject to proper process and protection, carriers make available to law enforcement personnel recorded information about their interactions with customers to aid their investigations.

III. THE COMMISSION SHOULD NOT MANDATE STANDARDS REGARDING THE PHYSICAL TRANSFER OF INFORMATION BETWEEN CARRIERS

The Commission should not adopt rules governing the physical transfer of information between carriers or between carriers and their affiliates and/or joint venture partners and independent contractors.[14] Carriers currently employ physical safeguards regarding the transfer of data that are unique and

---

Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended, 14 FCC Rcd 14409 (1999).

13 Reply Comments of the U.S. Department of Justice and the Federal Bureau of Investigation at 16 (Nov. 19, 2002).

14 FNPRM ¶ 70 (seeking comment on whether the Commission should adopt rules governing the physical transfer of CPNI among companies, such as between a carrier and its affiliate, or the transfer of CPNI to any other third party authorized to access or maintain CPNI, including a carrier's joint venture partners and independent contractors).

appropriate for their own companies and the particular situation (*e.g.*, transmission via a secure private channel, encrypted virtual private network, or shipment via a secure, traceable means). The record to date contains no evidence of unauthorized access to CPNI attributable to insufficiently protected physical transfers of CPNI. Moreover, the proposed requirement would impose significant costs and burdens on carriers and provide no measurable benefit in return.

IV. ADOPTING DATA RETENTION LIMITS COULD CONFLICT WITH EXISTING FEDERAL AND STATE DATA RETENTION RULES

The Commission should not adopt new data retention limitations and corresponding data destruction requirements applicable to CPNI.[15] The record to date does not indicate a need for such requirements and there is no reason to believe that such requirements would not create more problems than they help resolve, if adopted. Moreover, as the Commission indicated in the FNPRM, numerous states and the federal government (including the Commission)[16] already have adopted various data retention requirements. Adopting data destruction requirements likely would conflict with those data retention requirements. In addition, in response to the Commission's inquiry,[17] given the breadth of the various state and federal data retention rules, it would be virtually impossible to identify a subset of information that could be carved out from a carrier's records to be destroyed without conflicting with pre-existing regulations. Furthermore, limiting

15 *Id.* ¶ 71.

16 *See, e.g.,* 47 C.F.R. § 42.01-.11 (requiring carriers to maintain toll records for a specified period of time, and adopting other data retention requirements).

17 FNPRM ¶ 71.

the amount of time that a carrier could retain records (and thus mandating destruction of records after a specified period of time) potentially could impede a carrier's ability to protect itself in the event of a billing dispute or other carrier-customer or carrier-carrier dispute. Accordingly, the Commission should decline to adopt data retention limitations and destruction regulations specifically applicable to CPNI.

V. CONCLUSION

For the foregoing reasons, the Commission should not implement additional, burdensome, costly, frustrating and ineffective requirements, none of which have been demonstrated as necessary and, if adopted, would have limited to no value in enhancing already proven methods of preventing unauthorized access to CPNI.

Respectfully submitted,

/s/

John J. Heitmann
Jennifer M. Kashatus
Kelley Drye & Warren LLP
3050 K Street, NW, Suite 400
Washington, D.C. 20007
(202) 342-8400 (telephone)
jheitmann@kelleydrye.com
jkashatus@kelleydrye.com

Counsel to NuVox Communications and XO Communications, LLC

July 9, 2007

CERTIFICATE OF SERVICE

I hereby certify that on this 9th day of July, 2007, the foregoing Joint Comments of NuVox Communications and XO Communications was filed electronically through the FCC's Electronic Comments Filing System (ECFS) and copies were served on thee following as indicated:

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554
Marlene.dortch@fcc.gov
VIA ECFS

Janice Myles
Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
Room 5-C140
445 12th Street, SW
Washington, D.C. 20554
Janice.myles@fcc.gov
VIA ELECTRONIC MAIL

Adam Kirschenbaum, Esq.
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554
Adam.Kirschenbaum@fcc.gov
VIA ELECTRONIC MAIL

Best Copy & Printing, Inc. (BCPI)
Portals II
445 12th Street, S.W.
Room CY-B402
Washington, DC 20554
fcc@bcpiweb.com
VIA ELECTRONIC MAIL

/s/
Tara K. Mahoney